PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-074365
(43)Date of publication of application : 15.03.2002

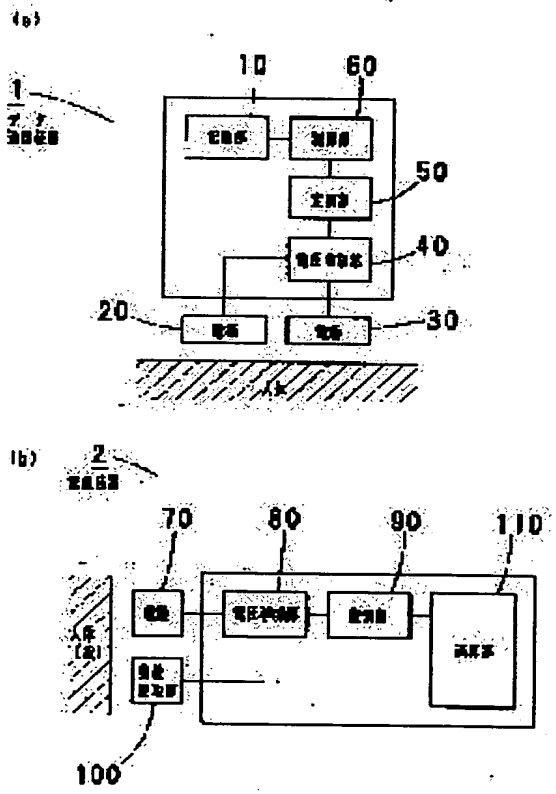
(51)Int.CI. G06T 7/00
A61B 5/117
G06F 1/00
G06F 15/00
G06T 1/00
H04L 9/32

(21)Application number : 2000-264346
(22)Date of filing : 31.08.2000

(71)Applicant : MATSUSHITA ELECTRIC WORKS LTD
(72)Inventor : DOI KANEYUKI
KOYAMA MASAKI
SUZUKI YOSHIKO
NISHIMURA ATSUHISA

(54) IDENTITY AUTHENTICATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an identity authentication system capable of performing identity authentication based on both the collation of data peculiar for a person and the collation of biological data (fingerprint data) with simple operation.
SOLUTION: The identity authentication is performed by a data communication equipment 1 for transmitting ID data and fingerprint data in a storage part 10 through two electrodes 20 and 30 located while facing the body of the person and an authentication device 2 for acquiring the ID data and the fingerprint data from a received signal through a receiving electrode 70 for receiving the signal from the data communication equipment 1 when the person touches the device, reading the fingerprint data of that person by having a fingerprint reading part 100, and performing the collation of the ID data and the collation of the fingerprint data.



LEGAL STATUS
[Date of request for examination] 15.07.2002

[Date of sending the examiner's decision of rejection]	13.07.2004
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

CLAIMS

[Claim(s)]
[Claim 1] In an authentication system collating of people's proper data, and collating of said man's living body data -- him -- him who attests -- The storage section which memorizes the fingerprint data as said man's proper data, and said man's living body data, two electrodes arranged so that said man's body may be faced -- this -- with the electrical-potential-difference impression section which impresses an electrical potential difference to inter-electrode [two] The data communication unit which has the control section which performs input/output control of the data of said storage section, and the modulation section which modulates the output signal from this control section, and outputs a modulating signal to said electrical-potential-difference impression section, The received electrode which receives the signal from said two electrodes, and the fingerprint read station which reads said man's fingerprint, While collating the electrical-potential-difference detecting element which detects the input signal of said received electrode, the recovery section which restores to the input signal detected by this electrical-potential-difference detecting element, and said proper data outputted from this recovery section and the registered proper data him who is characterized by collating said fingerprint data outputted from this recovery section, and the fingerprint data outputted from said fingerprint read station, and providing the authentication equipment which has the operation part which attests said man by the collating result of said proper data, and the collating result of said fingerprint data -- an authentication system.
[Claim 2] The electrical-potential-difference impression section which impresses an electrical potential difference between said received electrodes and circuit glands of said authentication equipment in said authentication equipment, the modulation section which modulates the signal from said operation part and outputs a modulating signal to this electrical-potential-difference impression section -- adding -- said data communication unit -- setting -- said two inter-electrode electrical potential differences of said data communication unit -- or While adding the electrical-potential-difference detecting element which detects the electrical potential difference of Hazama of one electrode of one of said two electrodes, and the circuit gland of said data communication unit, and the recovery section which restores to the signal detected by this electrical-potential-difference detecting element The he authentication system according to claim 1 characterized by having added the function to input the recovery data from this recovery section into said storage section to said control section, and enabling transmission of the data of said authentication equipment to said data communication unit.
[Claim 3] The he authentication system according to claim 1 or 2 characterized by preparing the constant current control section which controls said electrical-potential-difference impression section to become a predetermined value in said data communication unit about the amount of currents which flows to inter-electrode [said / two].
[Claim 4] The he authentication system according to claim 1 to 3 which it is the optical fingerprint read station in which said fingerprint read station reads a fingerprint with an optical means in said authentication equipment, and said received electrode is a transparent electrode, and is characterized by reading a fingerprint by said optical fingerprint read station through this transparent electrode.
[Claim 5] The he authentication system according to claim 1 to 4 characterized by being data with which the fingerprint data in said storage section were compressed.
[Claim 6] The he authentication system according to claim 1 to 5 characterized by the fingerprint data in said storage section being simplified data in which the description of a fingerprint is shown.

[Claim 7] The he authentication system according to claim 1 to 6 characterized by being data with which the fingerprint data in said storage section were enciphered.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] both biometrics according [this invention] to a fingerprint, and collating of individual proper data, such as ID data, -- him -- him who attests -- it is related with an authentication system.
[0002]
[Description of the Prior Art] it is represented by the ATM card -- as -- the former -- him -- the combination of a magnetic card and a recitation number is well used as a means which attests. However, comparatively simply, since reading is possible, forgery of a card is easy to be performed and a recitation number may also try to be stolen by the data recorded on the magnetic card at the time of an input. Moreover, since the personal identification number is using numeric values which he tends to memorize, such as a birthday, in many cases, a guess is also easy to be carried out. For this reason, it has been the problem that the criminal damage by systematic card counterfeiting is big.
[0003] Then, the memory card called the IC card in which the access restriction to a data encryption or data is possible has appeared. However, also in the case of an IC card, the theft of the real card is carried out, and the damage by so-called "spoofing" at the time of being used for others cannot be prevented.
[0004] on the other hand -- him -- as the completely different means of authentication -- every living bodies, such as recent years, a fingerprint, a voiceprint, and a retina, -- the description of a proper -- using -- him -- the biometrics (biometrics) which attest have been used. since "spoofing" is not made in biometrics -- him -- it is effective as a means of authentication. him who used the fingerprint also in it especially -- authentication precision is boiling an authentication system markedly and is improving, and since low-pricing is also progressing, the use range is expanding it.
[0005] however, him by biometrics -- since there is much (2) amount of data with it difficult [to make the rate of (1) he refusal and the rate of others acceptance into zero], there is a problem of ** which cannot perform an exchange of (3) data which require time amount for authentication processing in an authentication system. then, him who compensates a mutual fault and suits by using both data collatings and biometrics using an IC card -- the authentication system is proposed.
[0006]
[Problem(s) to be Solved by the Invention] however, him using both data collatings and biometrics using an IC card -- in an authentication system, in order to attest, it is necessary to perform separately completely different actuation of actuation of data collating in which the IC card was used, and the actuation for biometrics, and takes time and effort very much.
[0007] him this invention is what was made in view of the above-mentioned reason, and the place made into the purpose is easy actuation, and according to both people's proper data collating and living body data collating -- him who can attest -- it is in offering an authentication system.
[0008]
[Means for Solving the Problem] In order to attain the above-mentioned purpose, invention according to claim 1 In an authentication system collating of people's proper data, and collating of said man's living body data -- him -- him who attests -- The storage section which memorizes the fingerprint data as said man's proper data, and said man's living body data, two electrodes arranged so that said man's body may be faced -- this -- with the electrical-potential-difference impression section which impresses an electrical potential

difference to inter-electrode [two] The data communication unit which has the control section which performs input/output control of the data of said storage section, and the modulation section which modulates the output signal from this control section, and outputs a modulating signal to said electrical-potential-difference impression section, The received electrode which receives the signal from said two electrodes, and the fingerprint read station which reads said man's fingerprint, While collating the electrical-potential-difference detecting element which detects the input signal of said received electrode, the recovery section which restores to the input signal detected by this electrical-potential-difference detecting element, and said proper data outputted from this recovery section and the registered proper data It is characterized by collating said fingerprint data outputted from this recovery section, and the fingerprint data outputted from said fingerprint read station, and providing the authentication equipment which has the operation part which attests said man by the collating result of said proper data, and the collating result of said fingerprint data.

[0009] Invention according to claim 2 is a he authentication system according to claim 1, and is set to said authentication equipment. Add the electrical-potential-difference impression section which impresses an electrical potential difference between said received electrodes and circuit glands of said authentication equipment, and the modulation section which modulates the signal from said operation part and outputs a modulating signal to this electrical-potential-difference impression section, and it sets to said data communication unit. said two inter-electrode electrical potential differences of said data communication unit -- or While adding the electrical-potential-difference detecting element which detects the electrical potential difference between one electrode of one of said two electrodes, and the circuit gland of said data communication unit, and the recovery section which restores to the signal detected by this electrical-potential-difference detecting element It is characterized by having added the function to input the recovery data from this recovery section into said storage section to said control section, and enabling transmission of the data of said authentication equipment to said data communication unit.

[0010] Invention according to claim 3 is a he authentication system according to claim 1 or 2, and is characterized by preparing the constant current control section which controls said electrical-potential-difference impression section to become a predetermined value about the amount of currents which flows to inter-electrode [said / two] in said data communication unit.

[0011] It is a he authentication system according to claim 1 to 3, and in said authentication equipment, it is the optical fingerprint read station in which said fingerprint read station reads a fingerprint with an optical means, said received electrode is a transparent electrode, and invention according to claim 4 is characterized by reading a fingerprint by said optical fingerprint read station through this transparent electrode.

[0012] Invention according to claim 5 is characterized by being a he authentication system according to claim 1 to 4, and being data with which the fingerprint data in said storage section were compressed.

[0013] Invention according to claim 6 is characterized by being a he authentication system according to claim 1 to 5, and the fingerprint data in said storage section being simplified data in which the description of a fingerprint is shown.

[0014] Invention according to claim 7 is characterized by being a he authentication system according to claim 1 to 6, and being data with which the fingerprint data in said storage section were enciphered.

[0015]

[Embodiment of the Invention] him who starts the gestalt of operation of this invention hereafter -- an authentication system is explained based on drawing 1 thru/or drawing 5 .

[0016] drawing 1 -- him of the gestalt of operation of the 1st of this invention -- the block diagram showing an authentication system -- it is -- drawing 1 (a) -- him -- the block diagram and drawing 1 R> 1 (b) which show the data communication unit of an authentication system -- him -- it is the block diagram showing the authentication equipment of an authentication system.

[0017] As shown in drawing 1 (a), a data communication unit 1 The storage section 10 which memorizes the fingerprint data as a user's proper data (ID data) and this user's living body data, The electrical-potential-difference impression section 40 which impresses an electrical potential difference between the electrode 20 and electrode 30 which have been arranged so that a user's body may be faced, and this electrode 20 and an electrode 30, It comes to have the control section 60 which performs input/output control of the data of the storage section

10, and the modulation section 50 which modulates the output signal from a control section 60, and outputs a modulating signal to the electrical-potential-difference impression section 40. As shown in drawing 1 (b), moreover, authentication equipment 2 The received electrode 70 which receives the signal from the electrodes 20 and 30 of a data communication unit 1, The fingerprint read station 100 which reads a user's fingerprint, and the electrical-potential-difference detecting element 80 which detects the input signal of the received electrode 70, While collating the recovery section 90 which restores to the input signal detected by the electrical-potential-difference detecting element 80, and said ID data (ID data memorized by the storage section 10 of a data communication unit 1) outputted from the recovery section 90 and ID data registered beforehand Said fingerprint data (fingerprint data memorized by the storage section 10 of a data communication unit 1) outputted from the recovery section 90 and the fingerprint data outputted from the fingerprint read station 100 are collated. It comes to have the operation part 110 which attests a user by the collating result of ID data, and the collating result of fingerprint data.

[0018] Here, the part of the arbitration a user's body is equipped with a data communication unit 1, and as above-mentioned, electrodes 20 and 30 are installed so that a user's body may be faced. Authentication equipment 2 is touched by a user's Lord at a hand, the part or finger of a hand contacts the received electrode 70, and a user's finger contacts the fingerprint read station 100.

[0019] Next, actuation of he authentication is explained. If a user touches the received electrode 70 and the fingerprint read station 100 of authentication equipment 2, in a data communication unit 1, a user's ID data and fingerprint data which are memorized by the storage section 10 will be outputted by the control section 60, this output signal will be modulated in the modulation section 50, and this modulating signal will be transmitted through the electrical-potential-difference impression section 40, an electrode 20, and an electrode 30. With authentication equipment 2, the sending signal from a data communication unit 1 is received by the received electrode 70, this input signal is detected as a voltage signal by the electrical-potential-difference detecting element 80, it gets over in the recovery section 90, and this voltage signal is inputted into operation part 110. On the other hand, in the fingerprint read station 100, a user's fingerprint data are read and this fingerprint data is also inputted into operation part 110.

[0020] While collating ID data (ID data memorized by the storage section 10 of a data communication unit 1) contained in a sending signal from a data communication unit 1, and ID data beforehand registered into operation part 110 in operation part 110 It is outputted from the fingerprint data (fingerprint data memorized by the storage section 10 of a data communication unit 1) and the fingerprint read station 100 which are contained in this sending signal, and the ****** data inputted into operation part 110 are collated. Actuation which attests a user by the collating result of ID data and the collating result of fingerprint data is performed.

[0021] thus, the gestalt of the 1st operation -- setting -- collating of ID data, and collating of fingerprint data -- the mutual fault of a both collating means -- compensating -- suiting -- him, while being able to prevent reduction and "spoofing" of the rate of refusal, or the rate of others acceptance Since the communication link which made the body the transmission line is performing transmission of ID data from the data communication unit 1 to authentication equipment 2, and fingerprint data, the effectiveness that data transmission can be performed only by a user touching the received electrode 70 of authentication equipment 2 is done so. If the fingerprint read station 100 and the received electrode 70 are arranged in authentication equipment 2 so that it may approach mutually as especially shown in drawing 2 , a user can touch the fingerprint read station 100 and the received electrode 70 at coincidence, and can perform collating by ID data, and collating by fingerprint data to coincidence. therefore, collating according to ID data by very easy actuation and collating by fingerprint data -- him -- it can attest.

[0022] In addition, if attached to radical Motohara ** which transmits data from a data communication unit 1 by making the body into a transmission line to authentication equipment 2, it is the same as what is indicated by Japanese Patent Application No. No. 186005 [11 to] by the applicant for this patent.

[0023] moreover, him of the gestalt of this 1st operation -- an authentication system can be used for not only an alternative of an ATM card or a credit card but a close leaving managerial system, various keyless entry and a computer, the security of a personal digital assistant (a cellular phone is included), etc.

[0024] drawing 3 -- him of the gestalt of operation of the 2nd of this invention -- a showing

[an authentication system] block diagram -- it is -- drawing 3 (a) -- him -- the block diagram and drawing 3 (b) which show the data communication unit of an authentication system -- him -- it is the block diagram showing the authentication equipment of an authentication system.

[0025] As shown in drawing 3 (a), a data communication unit 1 the 1st configuration of the gestalt (drawing 1 (a)) of operation -- the electrical potential difference between the electrode 20 of a data communication unit 1, and an electrode 30 -- or While adding the electrical-potential-difference detecting element 45 which detects the electrical potential difference between one electrode of either an electrode 20 and the electrode 30, and the circuit gland of a data communication unit 1, and the recovery section 55 which restores to the signal detected by the electrical-potential-difference detecting element 45 The function to input the recovery data from the recovery section 55 into the storage section is added to a control section 60, and it enables it to receive the transmit data from authentication equipment 2. Moreover, said authentication equipment 2 adds the electrical-potential-difference impression section 85 which impresses an electrical potential difference between the received electrode 70 and the circuit gland of authentication equipment 2, and the modulation section 95 which modulates the signal from operation part 110 and outputs a modulating signal to the electrical-potential-difference impression section 85 to the 1st configuration of the gestalt (drawing 1 (b)) of operation, and enables it to transmit data to it from authentication equipment 2, as show in drawing 3 (b).

[0026] According to the configuration of the gestalt of this 2nd operation, if a user touches the received electrode 70 of authentication equipment 2, various kinds of data held or registered in the operation part 110 of authentication equipment 2 will be modulated in the modulation section 95, and this modulating signal will be transmitted through the electrical-potential-difference impression section 85 and the received electrode 70 (here, it is used for transmission). In a data communication unit 1, the sending signal from authentication equipment 2 is received by an electrode 20 and the electrode 30 (here, it is used for reception), this input signal is detected as a voltage signal by the electrical-potential-difference detecting element 45, it gets over in the recovery section 55, and this voltage signal is inputted into the storage section 10 by the control section 60. That is, in addition to actuation of the gestalt of the 1st operation, data transmission from authentication equipment 2 to a data communication unit 1 can also be performed. In other words, two-way communication of data can be performed in a data communication unit 1 and authentication equipment 2.

[0027] thus -- since two-way communication of data can be performed -- him -- after attesting, the effectiveness that various data can be exchanged between a data communication unit 1 and authentication equipment 2 is done so. thereby -- the exchange of important information, such as an exchange of cybermoney and an exchange of extra sensitive information, -- certain -- him -- after attesting, it comes to be able to do and is safe for a user. Moreover, the fingerprint data which read initial registration of the fingerprint data in a data communication unit 1 (storage section 10) with authentication equipment 2 (fingerprint read station 100) can be performed by transmitting to a data communication unit 1.

[0028] In addition, although he is trying to detect the electrical potential difference between the electrode 20 of a data communication unit 1, and an electrode 30 by the electrical-potential-difference detecting element 45, you may make it detect the electrical potential difference between the electrode of either an electrode 20 and the electrode 30, and the circuit gland of a data communication unit 1 with this operation gestalt. Moreover, if attached to radical Motohara ** which transmits data from authentication equipment 2 by making the body into a transmission line to a data communication unit 1, it is the same as what is indicated by Japanese Patent Application No. No. 339131 [11 to] by the applicant for this patent.

[0029] furthermore, him of the gestalt of the 2nd operation in which this bidirectional data transmission is possible -- an authentication system can be used for various applications currently assumed with the IC card, such as a settlement system by cybermoney, an electronic license, and an electronic health insurance card.

[0030] drawing 4 -- him of the gestalt of operation of the 3rd of this invention -- it is the block diagram showing the data communication unit of an authentication system. With this operation gestalt, the constant current control section 120 which controls the electrical-potential-difference value impressed to an electrode 20 and an electrode 30 is provided so that it may become the defined value with the amount of currents which flows between the electrode 20 of a data communication unit 1, and electrodes 30. The impedance

component of the interface of the body, the body, and an electrode changes with every individual and parts, and changes with conditions of the occasional skin also by the same person's same part. That is, even if it is performing the same electrical-potential-difference impression, the flowing amount of currents will change, and data communication becomes impossible when there are too much few the amounts of currents. Then, the difference by the individual, the part, a skin condition, etc. can be absorbed now by forming the constant current control section 120 which controls an electrical-potential-difference value so that it may become the defined value which has the amount of currents which flows between an electrode 20 and electrodes 30 in the electrical-potential-difference impression section 40, and the data communication stabilized more becomes possible. Moreover, control of such an applied-voltage value is important also from a viewpoint of safety. That is, if not much many currents flow the body, since it is dangerous, the safety to the body is securable here by setting up the current value within safe limits in the constant current control section 120.

[0031] In addition, although the constant current control section 120 is applied to the data communication unit 1 of the gestalt of the 2nd operation, you may apply to the data communication unit 1 of the gestalt of the 1st operation here.

[0032] drawing 5 -- him of the gestalt of operation of the 4th of this invention -- it is outline drawing of the authentication equipment of an authentication system. Transparent electrodes, such as ITO (Indium Tin Oxide: indium stannic acid ghost), are used for the received electrode 70 of authentication equipment 2, a fingerprint shall be read for the fingerprint read station 100 with an optical means, it arranges so that the received electrode 70 may be piled up on the fingerprint read station 100, and he is trying to read a fingerprint by the fingerprint read station 100 through the received electrode 70 (transparent electrode) with this operation gestalt. thus, by carrying out, both collating of ID data and collating of fingerprint data make to coincidence only by a user putting a finger on the fingerprint read station 100 -- having -- him -- it can attest.

[0033] furthermore, in the gestalt of each operation of this invention, it is good also as the data which compressed the fingerprint data which the storage section 10 of a data communication unit 1 is made to memorize, or simplified data in which the descriptions of a fingerprint, such as etc., branching -- breaking off -- are shown. By doing in this way, the amount of data of fingerprint data decreases and the time amount which memory space not only decreases, but data communication takes can also be shortened now. Moreover, it is good also as data which enciphered fingerprint data. By doing in this way, security nature can be made high more.

[0034]

[Effect of the Invention] In an authentication system according to [like / ****] invention of this invention according to claim 1 -- collating of people's proper data, and collating of said man's living body data -- him -- him who attests -- The storage section which memorizes the fingerprint data as said man's proper data, and said man's living body data, two electrodes arranged so that said man's body may be faced -- this -- with the electrical-potential-difference impression section which impresses an electrical potential difference to inter-electrode [two] The data communication unit which has the control section which performs input/output control of the data of said storage section, and the modulation section which modulates the output signal from this control section, and outputs a modulating signal to said electrical-potential-difference impression section, The received electrode which receives the signal from said two electrodes, and the fingerprint read station which reads said man's fingerprint, While collating the electrical-potential-difference detecting element which detects the input signal of said received electrode, the recovery section which restores to the input signal detected by this electrical-potential-difference detecting element, and said proper data outputted from this recovery section and the registered proper data Said fingerprint data outputted from this recovery section and the fingerprint data outputted from said fingerprint read station are collated. him according to both data collating and biometrics by easy actuation since the authentication equipment which has the operation part which attests said man by the collating result of said proper data and the collating result of said fingerprint data was provided -- him who can attest -- the authentication system was able to be offered.

[0035] The electrical-potential-difference impression section which impresses an electrical potential difference between said received electrodes and circuit glands of said authentication equipment in said authentication equipment in invention according to claim 2, the modulation section which modulates the signal from said operation part and outputs a modulating signal to this electrical-potential-difference impression section -- adding -- said

data communication unit -- setting -- said two inter-electrode electrical potential differences of said data communication unit -- or While adding the electrical-potential-difference detecting element which detects the electrical potential difference between one electrode of one of said two electrodes, and the circuit gland of said data communication unit, and the recovery section which restores to the signal detected by this electrical-potential-difference detecting element Since the function to input the recovery data from this recovery section into said storage section was added to said control section and transmission of the data of said authentication equipment to said data communication unit was enabled between a data communication unit and authentication equipment -- the two-way communication of data -- it can do -- him -- after attesting, the effectiveness that various data can be exchanged between a data communication unit and authentication equipment is done so.

[0036] since the constant current control section which control said electrical potential difference impression section by invention according to claim 3 to become a predetermined value in said data communication unit about the amount of currents which flow to inter-electrode [said / two] be prepared , the difference by the individual , the part , a skin condition , etc. can be absorb now , and if [both] the data communication stabilized more become possible , the effectiveness that the safety to the body be securable will be do so .

[0037] in invention according to claim 4, in said authentication equipment, since it is the optical fingerprint read station in which said fingerprint read station reads a fingerprint with an optical means, said received electrode is a transparent electrode and the fingerprint was read by said optical fingerprint read station through this transparent electrode, both collating of ID data and collating of fingerprint data make to coincidence only by a user putting a finger on a fingerprint read station -- having -- him -- the effectiveness that it can attest is done so.

[0038] In invention according to claim 5, since it is data with which the fingerprint data in said storage section were compressed, the amount of data of fingerprint data decreases and the effectiveness that the time amount which memory space not only decreases, but data communication takes can also be shortened is done so.

[0039] In invention according to claim 6, since the fingerprint data in said storage section are simplified data in which the description of a fingerprint is shown, the amount of data of fingerprint data decreases and the effectiveness that the time amount which memory space not only decreases, but data communication takes can also be shortened is done so.

[0040] In invention according to claim 7, since it is data with which the fingerprint data in said storage section were enciphered, the effectiveness that security nature can be made high more is done so.

[Translation done.]

TECHNICAL FIELD

[Field of the Invention] both biometrics according [this invention] to a fingerprint, and collating of individual proper data, such as ID data, -- him -- him who attests -- it is related with an authentication system.

[Translation done.]

PRIOR ART

[Description of the Prior Art] it is represented by the ATM card -- as -- the former -- him -- the combination of a magnetic card and a recitation number is well used as a means which attests. However, comparatively simply, since reading is possible, forgery of a card is easy to be performed and a recitation number may also try to be stolen by the data recorded on the magnetic card at the time of an input. Moreover, since the personal identification number is using numeric values which he tends to memorize, such as a birthday, in many cases, a guess is also easy to be carried out. For this reason, it has been the problem that the criminal damage by systematic card counterfeiting is big.
[0003] Then, the memory card called the IC card in which the access restriction to a data encryption or data is possible has appeared. However, also in the case of an IC card, the theft of the real card is carried out, and the damage by so-called "spoofing" at the time of being used for others cannot be prevented.
[0004] on the other hand -- him -- as the completely different means of authentication -- every living bodies, such as recent years, a fingerprint, a voiceprint, and a retina, -- the description of a proper -- using -- him -- the biometrics (biometrics) which attest have been used. since "spoofing" is not made in biometrics -- him -- it is effective as a means of authentication. him who used the fingerprint also in it especially -- authentication precision is boiling an authentication system markedly and is improving, and since low-pricing is also progressing, the use range is expanding it.
[0005] however, him by biometrics -- since there is much (2) amount of data with it difficult [to make the rate of (1) he refusal and the rate of others acceptance into zero], there is a problem of ** which cannot perform an exchange of (3) data which require time amount for authentication processing in an authentication system. then, him who compensates a mutual fault and suits by using both data collatings and biometrics using an IC card -- the authentication system is proposed.

[Translation done.]

EFFECT OF THE INVENTION

[Effect of the Invention] In an authentication system according to [like / ****] invention of this invention according to claim 1 -- collating of people's proper data, and collating of said man's living body data -- him -- him who attests -- The storage section which memorizes the fingerprint data as said man's proper data, and said man's living body data, two electrodes arranged so that said man's body may be faced -- this -- with the electrical-potential-difference impression section which impresses an electrical potential difference to inter-electrode [two] The data communication unit which has the control section which performs input/output control of the data of said storage section, and the modulation section which modulates the output signal from this control section, and outputs a modulating signal to said electrical-potential-difference impression section, The received electrode which receives the signal from said two electrodes, and the fingerprint read station which reads said man's fingerprint, While collating the electrical-potential-difference detecting element which detects the input signal of said received electrode, the recovery section which restores to the input signal detected by this electrical-potential-difference detecting element, and said proper data outputted from this recovery section and the registered proper data Said fingerprint data outputted from this recovery section and the fingerprint data outputted from said fingerprint read station are collated. him according to both data collating and biometrics by easy actuation since the authentication equipment which has the operation part which attests said man by the collating result of said proper data and the collating result of said fingerprint data was provided -- him who can attest -- the authentication system was able to be offered.
[0035] The electrical-potential-difference impression section which impresses an electrical potential difference between said received electrodes and circuit glands of said authentication equipment in said authentication equipment in invention according to claim 2, the modulation section which modulates the signal from said operation part and outputs a modulating signal to this electrical-potential-difference impression section -- adding -- said data communication unit -- setting -- said two inter-electrode electrical potential differences of said data communication unit -- or While adding the electrical-potential-difference detecting element which detects the electrical potential difference between one electrode of one of said two electrodes, and the circuit gland of said data communication unit, and the recovery section which restores to the signal detected by this electrical-potential-difference detecting element Since the function to input the recovery data from this recovery section into said storage section was added to said control section and transmission of the data of said authentication equipment to said data communication unit was enabled between a data communication unit and authentication equipment -- the two-way communication of data -- it can do -- him -- after attesting, the effectiveness that various data can be exchanged between a data communication unit and authentication equipment is done so.
[0036] since the constant current control section which control said electrical potential difference impression section by invention according to claim 3 to become a predetermined value in said data communication unit about the amount of currents which flow to inter-electrode [said / two] be prepared , the difference by the individual , the part , a skin condition , etc. can be absorb now , and if [both] the data communication stabilized more become possible , the effectiveness that the safety to the body be securable will be do so .
[0037] in invention according to claim 4, in said authentication equipment, since it is the optical fingerprint read station in which said fingerprint read station reads a fingerprint with an optical means, said received electrode is a transparent electrode and the fingerprint

was read by said optical fingerprint read station through this transparent electrode, both collating of ID data and collating of fingerprint data make to coincidence only by a user putting a finger on a fingerprint read station -- having -- him -- the effectiveness that it can attest is done so.

[0038] In invention according to claim 5, since it is data with which the fingerprint data in said storage section were compressed, the amount of data of fingerprint data decreases and the effectiveness that the time amount which memory space not only decreases, but data communication takes can also be shortened is done so.

[0039] In invention according to claim 6, since the fingerprint data in said storage section are simplified data in which the description of a fingerprint is shown, the amount of data of fingerprint data decreases and the effectiveness that the time amount which memory space not only decreases, but data communication takes can also be shortened is done so.

[0040] In invention according to claim 7, since it is data with which the fingerprint data in said storage section were enciphered, the effectiveness that security nature can be made high more is done so.

[Translation done.]

TECHNICAL PROBLEM

[Problem(s) to be Solved by the Invention] however, him using both data collatings and biometrics using an IC card -- in an authentication system, in order to attest, it is necessary to perform separately completely different actuation of actuation of data collating in which the IC card was used, and the actuation for biometrics, and takes time and effort very much.

[0007] him this invention is what was made in view of the above-mentioned reason, and the place made into the purpose is easy actuation, and according to both people's proper data collating and living body data collating -- him who can attest -- it is in offering an authentication system.

[Translation done.]

MEANS

[Means for Solving the Problem] In order to attain the above-mentioned purpose, invention according to claim 1 In an authentication system collating of people's proper data, and collating of said man's living body data -- him -- him who attests -- The storage section which memorizes the fingerprint data as said man's proper data, and said man's living body data, two electrodes arranged so that said man's body may be faced -- this -- with the electrical-potential-difference impression section which impresses an electrical potential difference to inter-electrode [two] The data communication unit which has the control section which performs input/output control of the data of said storage section, and the modulation section which modulates the output signal from this control section, and outputs a modulating signal to said electrical-potential-difference impression section, The received electrode which receives the signal from said two electrodes, and the fingerprint read station which reads said man's fingerprint, While collating the electrical-potential-difference detecting element which detects the input signal of said received electrode, the recovery section which restores to the input signal detected by this electrical-potential-difference detecting element, and said proper data outputted from this recovery section and the registered proper data It is characterized by collating said fingerprint data outputted from this recovery section, and the fingerprint data outputted from said fingerprint read station, and providing the authentication equipment which has the operation part which attests said man by the collating result of said proper data, and the collating result of said fingerprint data.

[0009] Invention according to claim 2 is a he authentication system according to claim 1, and is set to said authentication equipment. Add the electrical-potential-difference impression section which impresses an electrical potential difference between said received electrodes and circuit glands of said authentication equipment, and the modulation section which modulates the signal from said operation part and outputs a modulating signal to this electrical-potential-difference impression section, and it sets to said data communication unit. said two inter-electrode electrical potential differences of said data communication unit -- or While adding the electrical-potential-difference detecting element which detects the electrical potential difference of Hazama of one electrode of one of said two electrodes, and the circuit gland of said data communication unit, and the recovery section which restores to the signal detected by this electrical-potential-difference detecting element It is characterized by having added the function to input the recovery data from this recovery section into said storage section to said control section, and enabling transmission of the data of said authentication equipment to said data communication unit.

[0010] Invention according to claim 3 is a he authentication system according to claim 1 or 2, and is characterized by preparing the constant current control section which controls said electrical-potential-difference impression section to become a predetermined value about the amount of currents which flows to inter-electrode [said / two] in said data communication unit.

[0011] It is a he authentication system according to claim 1 to 3, and in said authentication equipment, it is the optical fingerprint read station in which said fingerprint read station reads a fingerprint with an optical means, said received electrode is a transparent electrode, and invention according to claim 4 is characterized by reading a fingerprint by said optical fingerprint read station through this transparent electrode.

[0012] Invention according to claim 5 is characterized by being a he authentication system according to claim 1 to 4, and being data with which the fingerprint data in said storage section were compressed.

[0013] Invention according to claim 6 is characterized by being a he authentication system

according to claim 1 to 5, and the fingerprint data in said storage section being simplified data in which the description of a fingerprint is shown.
[0014] Invention according to claim 7 is characterized by being a he authentication system according to claim 1 to 6, and being data with which the fingerprint data in said storage section were enciphered.
[0015]
[Embodiment of the Invention] him who starts the gestalt of operation of this invention hereafter -- an authentication system is explained based on drawing 1 thru/or drawing 5 .
[0016] drawing 1 -- him of the gestalt of operation of the 1st of this invention -- the block diagram showing an authentication system -- it is -- drawing 1 (a) -- him -- the block diagram and drawing 1 R> 1 (b) which show the data communication unit of an authentication system -- him -- it is the block diagram showing the authentication equipment of an authentication system.
[0017] As shown in drawing 1 (a), a data communication unit 1 The storage section 10 which memorizes the fingerprint data as a user's proper data (ID data) and this user's living body data, The electrical-potential-difference impression section 40 which impresses an electrical potential difference between the electrode 20 and electrode 30 which have been arranged so that a user's body may be faced, and this electrode 20 and an electrode 30, It comes to have the control section 60 which performs input/output control of the data of the storage section 10, and the modulation section 50 which modulates the output signal from a control section 60, and outputs a modulating signal to the electrical-potential-difference impression section 40. As shown in drawing 1 (b), moreover, authentication equipment 2 The received electrode 70 which receives the signal from the electrodes 20 and 30 of a data communication unit 1, The fingerprint read station 100 which reads a user's fingerprint, and the electrical-potential-difference detecting element 80 which detects the input signal of the received electrode 70, While collating the recovery section 90 which restores to the input signal detected by the electrical-potential-difference detecting element 80, and said ID data (ID data memorized by the storage section 10 of a data communication unit 1) outputted from the recovery section 90 and ID data registered beforehand Said fingerprint data (fingerprint data memorized by the storage section 10 of a data communication unit 1) outputted from the recovery section 90 and the fingerprint data outputted from the fingerprint read station 100 are collated. It comes to have the operation part 110 which attests a user by the collating result of ID data, and the collating result of fingerprint data.
[0018] Here, the part of the arbitration a user's body is equipped with a data communication unit 1, and as above-mentioned, electrodes 20 and 30 are installed so that a user's body may be faced. Authentication equipment 2 is touched by a user's Lord at a hand, the part or finger of a hand contacts the received electrode 70, and a user's finger contacts the fingerprint read station 100.
[0019] Next, actuation of he authentication is explained. If a user touches the received electrode 70 and the fingerprint read station 100 of authentication equipment 2, in a data communication unit 1, a user's ID data and fingerprint data which are memorized by the storage section 10 will be outputted by the control section 60, this output signal will be modulated in the modulation section 50, and this modulating signal will be transmitted through the electrical-potential-difference impression section 40, an electrode 20, and an electrode 30. With authentication equipment 2, the sending signal from a data communication unit 1 is received by the received electrode 70, this input signal is detected as a voltage signal by the electrical-potential-difference detecting element 80, it gets over in the recovery section 90, and this voltage signal is inputted into operation part 110. On the other hand, in the fingerprint read station 100, a user's fingerprint data are read and this fingerprint data is also inputted into operation part 110.
[0020] While collating ID data (ID data memorized by the storage section 10 of a data communication unit 1) contained in a sending signal from a data communication unit 1, and ID data beforehand registered into operation part 110 in operation part 110 It is outputted from the fingerprint data (fingerprint data memorized by the storage section 10 of a data communication unit 1) and the fingerprint read station 100 which are contained in this sending signal, and the ****** data inputted into operation part 110 are collated. Actuation which attests a user by the collating result of ID data and the collating result of fingerprint data is performed.
[0021] thus, the gestalt of the 1st operation -- setting -- collating of ID data, and collating of fingerprint data -- the mutual fault of a both collating means -- compensating -- suiting -- him, while being able to prevent reduction and "spoofing" of the rate of refusal,

or the rate of others acceptance Since the communication link which made the body the transmission line is performing transmission of ID data from the data communication unit 1 to authentication equipment 2, and fingerprint data, the effectiveness that data transmission can be performed only by a user touching the received electrode 70 of authentication equipment 2 is done so. If the fingerprint read station 100 and the received electrode 70 are arranged in authentication equipment 2 so that it may approach mutually as especially shown in drawing 2 , a user can touch the fingerprint read station 100 and the received electrode 70 at coincidence, and can perform collating by ID data, and collating by fingerprint data to coincidence. therefore, collating according to ID data by very easy actuation and collating by fingerprint data -- him -- it can attest.

[0022] In addition, if attached to radical Motohara ** which transmits data from a data communication unit 1 by making the body into a transmission line to authentication equipment 2, it is the same as what is indicated by Japanese Patent Application No. No. 186005 [11 to] by the applicant for this patent.

[0023] moreover, him of the gestalt of this 1st operation -- an authentication system can be used for not only an alternative of an ATM card or a credit card but a close leaving managerial system, various keyless entry and a computer, the security of a personal digital assistant (a cellular phone is included), etc.

[0024] drawing 3 -- him of the gestalt of operation of the 2nd of this invention -- a showing [an authentication system] block diagram -- it is -- drawing 3 (a) -- him -- the block diagram and drawing 3 (b) which show the data communication unit of an authentication system -- him -- it is the block diagram showing the authentication equipment of an authentication system.

[0025] As shown in drawing 3 (a), a data communication unit 1 the 1st configuration of the gestalt (drawing 1 (a)) of operation -- the electrical potential difference of Hazama of the electrode 20 of a data communication unit 1, and an electrode 30 -- or While adding the electrical-potential-difference detecting element 45 which detects the electrical potential difference of Hazama of one electrode of either an electrode 20 and the electrode 30, and the circuit gland of a data communication unit 1, and the recovery section 55 which restores to the signal detected by the electrical-potential-difference detecting element 45 The function to input the recovery data from the recovery section 55 into the storage section is added to a control section 60, and it enables it to receive the transmit data from authentication equipment 2. Moreover, said authentication equipment 2 adds the electrical-potential-difference impression section 85 which impresses an electrical potential difference between the received electrode 70 and the circuit gland of authentication equipment 2, and the modulation section 95 which modulates the signal from operation part 110 and outputs a modulating signal to the electrical-potential-difference impression section 85 to the 1st configuration of the gestalt (drawing 1 (b)) of operation, and enables it to transmit data to it from authentication equipment 2, as show in drawing 3 (b).

[0026] According to the configuration of the gestalt of this 2nd operation, if a user touches the received electrode 70 of authentication equipment 2, various kinds of data held or registered in the operation part 110 of authentication equipment 2 will be modulated in the modulation section 95, and this modulating signal will be transmitted through the electrical-potential-difference impression section 85 and the received electrode 70 (here, it is used for transmission). In a data communication unit 1, the sending signal from authentication equipment 2 is received by an electrode 20 and the electrode 30 (here, it is used for reception), this input signal is detected as a voltage signal by the electrical-potential-difference detecting element 45, it gets over in the recovery section 55, and this voltage signal is inputted into the storage section 10 by the control section 60. That is, in addition to actuation of the gestalt of the 1st operation, data transmission from authentication equipment 2 to a data communication unit 1 can also be performed. In other words, two-way communication of data can be performed in a data communication unit 1 and authentication equipment 2.

[0027] thus -- since two-way communication of data can be performed -- him -- after attesting, the effectiveness that various data can be exchanged by Hazama of a data communication unit 1 and authentication equipment 2 is done so. thereby -- the exchange of important information, such as an exchange of cybermoney and an exchange of extra sensitive information, -- certain -- him -- after attesting, it comes to be able to do and is safe for a user. Moreover, the fingerprint data which read initial registration of the fingerprint data in a data communication unit 1 (storage section 10) with authentication equipment 2 (fingerprint read station 100) can be performed by transmitting to a data communication unit 1.

[0028] In addition, although he is trying to detect the electrical potential difference of Hazama with the electrode 20 of a data communication unit 1, and an electrode 30 by the electrical-potential-difference detecting element 45, you may make it detect the electrical potential difference of Hazama of the electrode of either an electrode 20 and the electrode 30, and the circuit gland of a data communication unit 1 with this operation gestalt. Moreover, if attached to radical Motohara ** which transmits data from authentication equipment 2 by making the body into a transmission line to a data communication unit 1, it is the same as what is indicated by Japanese Patent Application No. No. 339131 [11 to] by the applicant for this patent.

[0029] furthermore, him of the gestalt of the 2nd operation in which this bidirectional data transmission is possible -- an authentication system can be used for various applications currently assumed with the IC card, such as a settlement system by cybermoney, an electronic license, and an electronic health insurance card.

[0030] drawing 4 -- him of the gestalt of operation of the 3rd of this invention -- it is the block diagram showing the data communication unit of an authentication system. With this operation gestalt, the constant current control section 120 which controls the electrical-potential-difference value impressed to an electrode 20 and an electrode 30 is provided so that it may become the defined value with the amount of currents which flows between the electrode 20 of a data communication unit 1, and electrodes 30. The impedance component of the interface of the body, the body, and an electrode changes with every individual and parts, and changes with conditions of the occasional skin also by the same person's same part. That is, even if it is performing the same electrical-potential-difference impression, the flowing amount of currents will change, and data communication becomes impossible when there are too much few the amounts of currents. Then, the difference by the individual, the part, a skin condition, etc. can be absorbed now by forming the constant current control section 120 which controls an electrical-potential-difference value so that it may become the defined value which has the amount of currents which flows between an electrode 20 and electrodes 30 in the electrical-potential-difference impression section 40, and the data communication stabilized more becomes possible. Moreover, control of such an applied-voltage value is important also from a viewpoint of safety. That is, if not much many currents flow the body, since it is dangerous, the safety to the body is securable here by setting up the current value within safe limits in the constant current control section 120.

[0031] In addition, although the constant current control section 120 is applied to the data communication unit 1 of the gestalt of the 2nd operation, you may apply to the data communication unit 1 of the gestalt of the 1st operation here.

[0032] drawing 5 -- him of the gestalt of operation of the 4th of this invention -- it is outline drawing of the authentication equipment of an authentication system. Transparent electrodes, such as ITO (Indium Tin Oxide: indium stannic acid ghost), are used for the received electrode 70 of authentication equipment 2, a fingerprint shall be read for the fingerprint read station 100 with an optical means, it arranges so that the received electrode 70 may be piled up on the fingerprint read station 100, and he is trying to read a fingerprint by the fingerprint read station 100 through the received electrode 70 (transparent electrode) with this operation gestalt. thus, by carrying out, both collating of ID data and collating of fingerprint data make to coincidence only by a user putting a finger on the fingerprint read station 100 -- having -- him -- it can attest.

[0033] furthermore, in the gestalt of each operation of this invention, it is good also as the data which compressed the fingerprint data which the storage section 10 of a data communication unit 1 is made to memorize, or simplified data in which the descriptions of a fingerprint, such as etc., branching -- breaking off -- are shown. By doing in this way, the amount of data of fingerprint data decreases and the time amount which memory space not only decreases, but data communication takes can also be shortened now. Moreover, it is good also as data which enciphered fingerprint data. By doing in this way, security nature can be made high more.

[Translation done.]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] him of the gestalt of operation of the 1st of this invention -- it is the block diagram showing an authentication system, and (a) is the block diagram showing a data communication unit, and (b) is the block diagram showing authentication equipment.

[Drawing 2] It is outline drawing of the authentication equipment concerning the gestalt of operation of this invention.

[Drawing 3] him of the gestalt of operation of the 2nd of this invention -- it is the block diagram showing an authentication system, and (a) is the block diagram showing a data communication unit, and (b) is the block diagram showing authentication equipment.

[Drawing 4] him of the gestalt of operation of the 3rd of this invention -- it is the block diagram showing the data communication unit of an authentication system.

[Drawing 5] him of the gestalt of operation of the 4th of this invention -- it is outline drawing of the authentication equipment of an authentication system.

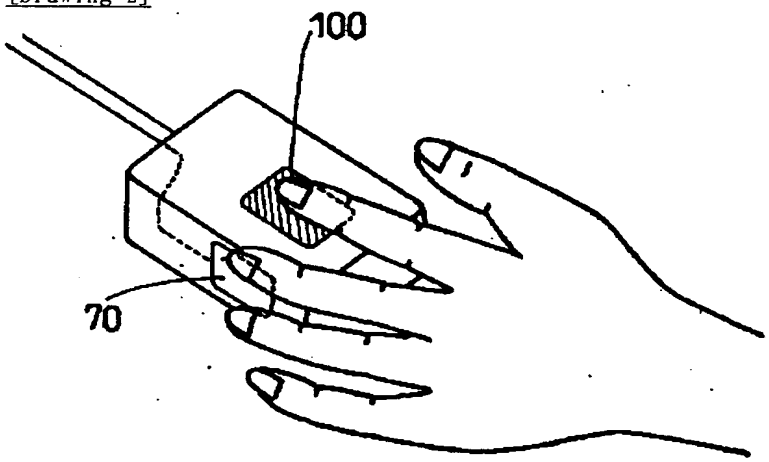
[Description of Notations]

1 Data Communication Unit
2 Authentication
10 Storage Section
20 Electrode
30 Electrode
40 Electrical-Potential-Difference Impression Section
45 Electrical-Potential-Difference Detecting Element
50 Modulation Section
55 Recovery Section
60 Control Section
70 Received Electrode
80 Electrical-Potential-Difference Detecting Element
85 Electrical-Potential-Difference Impression Section
90 Recovery Section
95 Modulation Section
100 Fingerprint Read Station
110 Operation Part
120 Constant Current Control Section

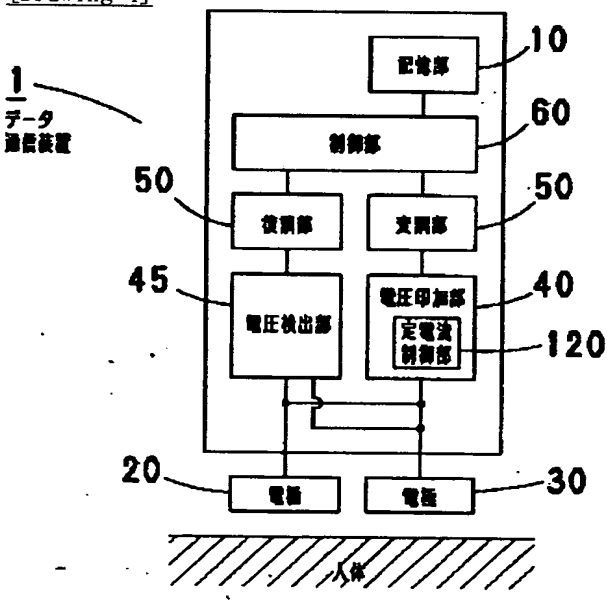
[Translation done.]

DRAWINGS

[Drawing 2]

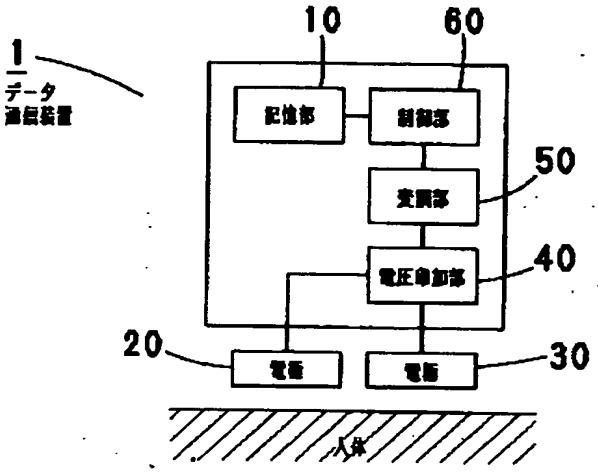


[Drawing 4]

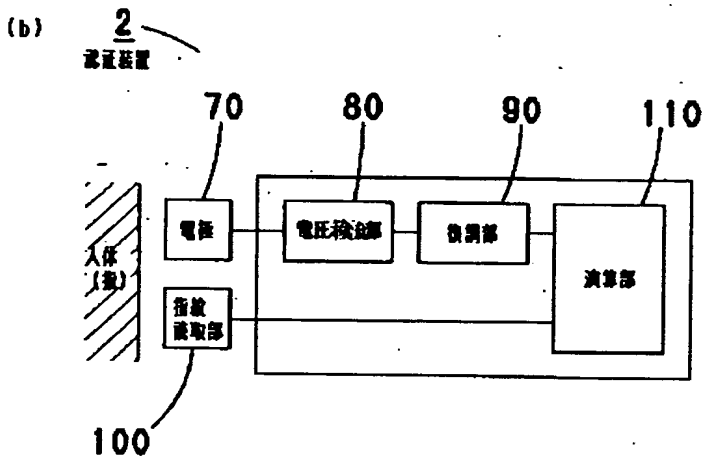


[Drawing 1]

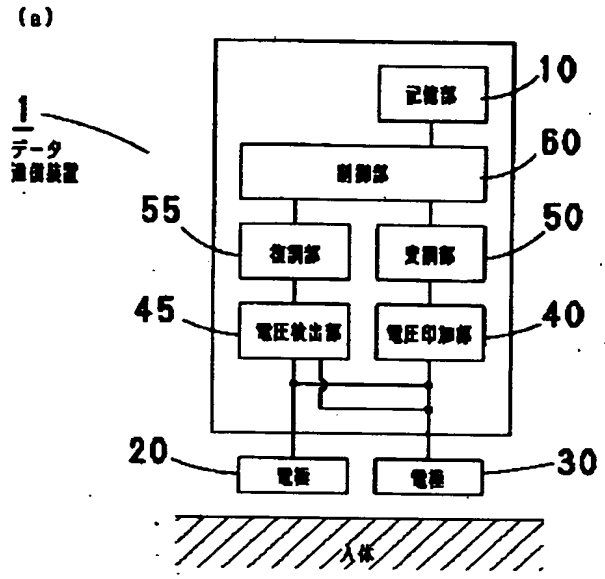
(a)


1
データ
通信装置
10
60
記憶部
制御部
50
変調部
40
電圧印加部
20
電極
電極
30
人体

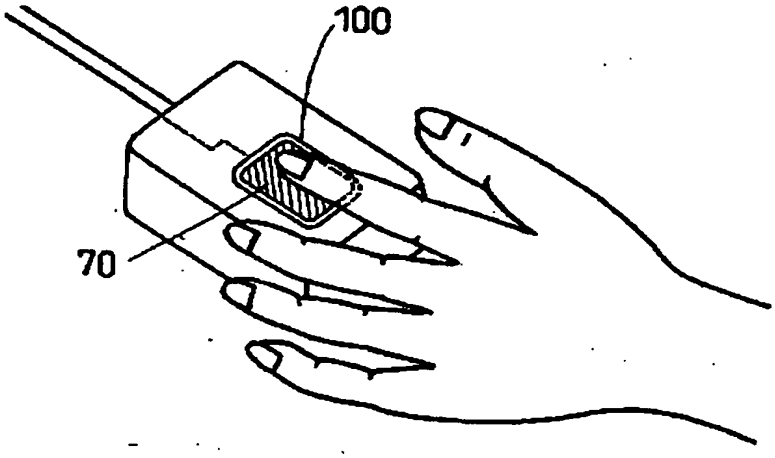
(b)


2
認証装置
70
80
90
110
電極
電圧検出部
制御部
演算部
人体
(指)
指紋
画取部
100

[Drawing 3]



[Drawing 5]



[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－74365
（P2002－74365A）
(43)公開日　平成14年３月15日(2002.3.15)

(51)Int.Cl.'		識別記号	FI			テーマコード(参考)
G06T	7/00	530	G06T	7/00	530	4C038
A61B	5/117		G06F	1/00	370E	5B043
G06F	1/00	370		15/00	330A	5B047
	15/00	330	G06T	1/00	400G	5B085
G06T	1/00	400	A61B	5/10	322	5J104

審査請求　未請求　請求項の数７　ＯＬ　（全８頁）　最終頁に続く

(21)出願番号　特願2000－264346(P2000－264346)

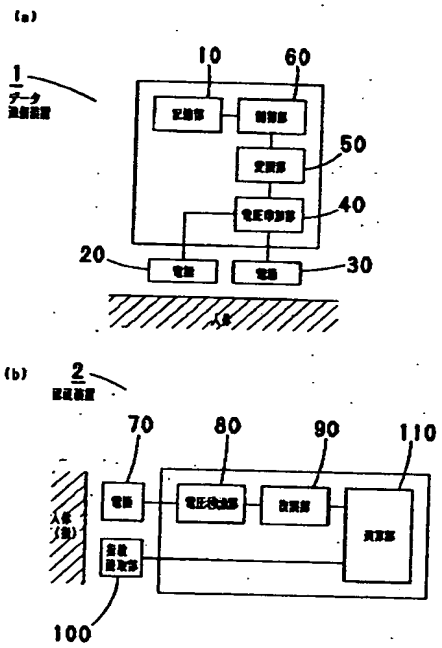
(22)出願日　平成12年８月31日(2000.8.31)

(71)出願人　000005832
松下電工株式会社
大阪府門真市大字門真1048番地
(72)発明者　▲土▼井　譲之
大阪府門真市大字門真1048番地松下電工株式会社内
(72)発明者　小山　正樹
大阪府門真市大字門真1048番地松下電工株式会社内
(74)代理人　100111556
弁理士　安藤　淳二　（外１名）

最終頁に続く

(54)【発明の名称】　本人認証システム

(57)【要約】
【課題】　簡単な操作で、人の固有データ照合と生体データ（指紋データ）照合の両方による本人認証を行うことができる本人認証システムを提供すること。
【解決手段】　記憶部１０のＩＤデータ及び指紋データを人の体に面するように配置した２つの電極２０，３０を介して送信するデータ通信装置１と、人が触れたときにデータ通信装置１からの信号を受信する受信電極７０を介してその受信信号からＩＤデータ及び指紋データを取得するとともに、指紋読取部１００を有して本人の指紋データを読み取り、ＩＤデータの照合と指紋データの照合を行う認証装置２とにより本人認証を行うことを特徴とする。



【特許請求の範囲】

【請求項１】　人の固有データの照合と前記人の生体データの照合とにより本人認証を行う本人認証システムにおいて、前記人の固有データ及び前記人の生体データとしての指紋データを記憶する記憶部と、前記人の体に面するように配置した２つの電極と、該２つの電極間に電圧を印加する電圧印加部と、前記記憶部のデータの入出力制御を行う制御部と、該制御部からの出力信号を変調し前記電圧印加部に変調信号を出力する変調部とを有するデータ通信装置と、前記２つの電極からの信号を受信する受信電極と、前記人の指紋を読み取る指紋読取部と、前記受信電極の受信信号を検出する電圧検出部と、該電圧検出部で検出された受信信号を復調する復調部と、該復調部から出力される前記固有データと登録された固有データとを照合するとともに、該復調部から出力される前記指紋データと前記指紋読取部から出力される指紋データとを照合して、前記固有データの照合結果と前記指紋データの照合結果とにより前記人を認証する演算部を有する認証装置とを具備することを特徴とする本人認証システム。

【請求項２】前記認証装置において、前記受信電極と前記認証装置の回路グランドとの間に電圧を印加する電圧印加部と、前記演算部からの信号を変調し該電圧印加部に変調信号を出力する変調部とを付加し、前記データ通信装置において、前記データ通信装置の前記２つの電極間の電圧もしくは、前記２つの電極のいずれかの一方の電極と前記データ通信装置の回路グランドとの間の電圧を検出する電圧検出部と、該電圧検出部で検出した信号を復調する復調部とを付加するとともに、前記制御部には該復調部からの復調データを前記記憶部に入力する機能を付加して、前記認証装置のデータを前記データ通信装置に伝送可能としたことを特徴とする請求項１記載の本人認証システム。

【請求項３】前記データ通信装置において、前記２つの電極間に流れる電流量を所定の値になるように前記電圧印加部を制御する定電流制御部を設けたことを特徴とする請求項１又は請求項２記載の本人認証システム。

【請求項４】前記認証装置において、前記指紋読取部が光学的手段により指紋を読み取る光学式指紋読取部であり、前記受信電極が透明電極であり、該透明電極を介して、前記光学式指紋読取部で指紋を読み取るようにしたことを特徴とする請求項１乃至請求項３のいずれかに記載の本人認証システム。

【請求項５】前記記憶部における指紋データが圧縮されたデータであることを特徴とする請求項１乃至請求項４のいずれかに記載の本人認証システム。

【請求項６】前記記憶部における指紋データが指紋の特徴を示す簡易化されたデータであることを特徴とする請求項１乃至請求項５のいずれかに記載の本人認証システム。

【請求項７】前記記憶部における指紋データが暗号化されたデータであることを特徴とする請求項１乃至請求項６のいずれかに記載の本人認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、指紋による生体認証と、ＩＤデータなど個人の固有データの照合との両方で本人認証を行う本人認証システムに関するものである。

【０００２】

【従来の技術】キャッシュカードに代表されるように、従来本人認証を行う手段として、磁気カードと暗唱番号の組み合わせがよく用いられている。しかし磁気カードに記録されたデータは比較的簡単に読み取りが可能であるため、カードの偽造が行われ易く、暗唱番号も入力時に盗み見られてしまう場合がある。また暗証番号は誕生日等の本人が覚えやすい数値を使用していることが多いため、推測もされやすい。このため組織的なカード偽造による犯罪被害が大きな問題となっている。

【０００３】そこで、データの暗号化やデータへのアクセス制限が可能なＩＣカードと呼ばれるメモリカードが登場している。ところが、ＩＣカードの場合でも、本物のカードが盗難され、他人に使用された場合の所謂「なりすまし」による被害は防ぐことができない。

【０００４】一方、本人認証の全く別の手段として、近年、指紋や声紋，網膜等、生体毎に固有の特徴を用いて本人認証を行う生体認証（バイオメトリックス）が実用されてきている。生体認証では「なりすまし」ができないため、本人認証の手段として有効である。特に、その中でも指紋を用いた本人認証システムは、認証精度が格段に向上してきており、低価格化も進んでいるため利用範囲が拡大してきている。

【０００５】しかし、生体認証による本人認証システムには、（１）本人拒否率や他人受入率をゼロにすることが困難である、（２）データ量が多いため認証処理に時間がかかる、（３）データのやりとりができない、等の問題がある。そこで、ＩＣカードを用いたデータ照合と生体認証の両方を用いることにより、互いの欠点を補いあう本人認証システムが提案されている。

【０００６】

【発明が解決しようとする課題】しかしながら、ＩＣカードを用いたデータ照合と生体認証の両方を用いる本人認証システムでは、認証するために、ＩＣカードを用いたデータ照合の操作と、生体認証のための操作という全く異なる操作を別々に行う必要があり、非常に手間がかかる。

【０００７】本発明は、上記事由に鑑みてなしたもので、その目的とするところは、簡単な操作で、人の固有データ照合と生体データ照合の両方による本人認証を行うことができる本人認証システムを提供することにあ

る。

【０００８】

【課題を解決するための手段】上記目的を達成するために、請求項１記載の発明は、人の固有データの照合と前記人の生体データの照合とにより本人認証を行う本人認証システムにおいて、前記人の固有データ及び前記人の生体データとしての指紋データを記憶する記憶部と、前記人の体に面するように配置した２つの電極と、該２つの電極間に電圧を印加する電圧印加部と、前記記憶部のデータの入出力制御を行う制御部と、該制御部からの出力信号を変調し前記電圧印加部に変調信号を出力する変調部とを有するデータ通信装置と、前記２つの電極からの信号を受信する受信電極と、前記人の指紋を読み取る指紋読取部と、前記受信電極の受信信号を検出する電圧検出部と、該電圧検出部で検出された受信信号を復調する復調部と、該復調部から出力される前記固有データと登録された固有データとを照合するとともに、該復調部から出力される前記指紋データと前記指紋読取部から出力される指紋データとを照合して、前記固有データの照合結果と前記指紋データの照合結果とにより前記人を認証する演算部を有する認証装置とを具備することを特徴とするものである。

【０００９】請求項２記載の発明は、請求項１記載の本人認証システムで、前記認証装置において、前記受信電極と前記認証装置の回路グランドとの間に電圧を印加する電圧印加部と、前記演算部からの信号を変調し該電圧印加部に変調信号を出力する変調部とを付加し、前記データ通信装置において、前記データ通信装置の前記２つの電極間の電圧もしくは、前記２つの電極のいずれかの一方の電極と前記データ通信装置の回路グランドとの間の電圧を検出する電圧検出部と、該電圧検出部で検出した信号を復調する復調部とを付加するとともに、前記制御部には該復調部からの復調データを前記記憶部に入力する機能を付加して、前記認証装置のデータを前記データ通信装置に伝送可能としたことを特徴とするものである。

【００１０】請求項３記載の発明は、請求項１又は請求項２記載の本人認証システムで、前記データ通信装置において、前記２つの電極間に流れる電流量を所定の値になるように前記電圧印加部を制御する定電流制御部を設けたことを特徴とするものである。

【００１１】請求項４記載の発明は、請求項１乃至請求項３のいずれかに記載の本人認証システムで、前記認証装置において、前記指紋読取部が光学的手段により指紋を読み取る光学式指紋読取部であり、前記受信電極が透明電極であり、該透明電極を介して、前記光学式指紋読取部で指紋を読み取るようにしたことを特徴とするものである。

【００１２】請求項５記載の発明は、請求項１乃至請求項４のいずれかに記載の本人認証システムで、前記記憶部における指紋データが圧縮されたデータであることを特徴とするものである。

【００１３】請求項６記載の発明は、請求項１乃至請求項５のいずれかに記載の本人認証システムで、前記記憶部における指紋データが指紋の特徴を示す簡易化されたデータであることを特徴とするものである。

【００１４】請求項７記載の発明は、請求項１乃至請求項６のいずれかに記載の本人認証システムで、前記記憶部における指紋データが暗号化されたデータであることを特徴とするものである。

【００１５】

【発明の実施の形態】以下、本発明の実施の形態に係る本人認証システムについて図１乃至図５にもとづき説明する。

【００１６】図１は、本発明の第１の実施の形態の本人認証システムを示すブロック図であり、図１（ａ）は本人認証システムのデータ通信装置を示すブロック図、図１（ｂ）は本人認証システムの認証装置を示すブロック図である。

【００１７】図１（ａ）に示すごとく、データ通信装置１は、使用者の固有データ（ＩＤデータ）及び同使用者の生体データとしての指紋データを記憶する記憶部１０と、使用者の体に面するように配置した電極２０及び電極３０と、この電極２０及び電極３０の間に電圧を印加する電圧印加部４０と、記憶部１０のデータの入出力制御を行う制御部６０と、制御部６０からの出力信号を変調し電圧印加部４０に変調信号を出力する変調部５０とを有してなる。また図１（ｂ）に示すごとく、認証装置２は、データ通信装置１の電極２０及び３０からの信号を受信する受信電極７０と、使用者の指紋を読み取る指紋読取部１００と、受信電極７０の受信信号を検出する電圧検出部８０と、電圧検出部８０で検出された受信信号を復調する復調部９０と、復調部９０から出力される前記ＩＤデータ（データ通信装置１の記憶部１０に記憶されていたＩＤデータ）と予め登録されたＩＤデータとを照合するとともに、復調部９０から出力される前記指紋データ（データ通信装置１の記憶部１０に記憶されていた指紋データ）と指紋読取部１００から出力される指紋データとを照合して、ＩＤデータの照合結果と指紋データの照合結果とにより使用者を認証する演算部１１０を有してなる。

【００１８】ここで、データ通信装置１は使用者の体の任意の箇所に装着されるものであり、前述のとおり電極２０及び３０は使用者の体に面するように設置される。認証装置２は使用者の主に手に触れられるもので、受信電極７０には手の一部又は指が接触し、指紋読取部１００には使用者の指が接触する。

【００１９】次に本人認証の動作について説明する。使用者が認証装置２の受信電極７０及び指紋読取部１００に触れると、データ通信装置１において、記憶部１０に

記憶されている使用者のＩＤデータ及び指紋データが、制御部6.0により出力されこの出力信号が変調部５０で変調され、この変調信号が電圧印加部４０と電極２０及び電極３０を介して送信される。認証装置２では、データ通信装置１からの送信信号が受信電極７０で受信され、この受信信号は電圧検出部８０で電圧信号として検出され、この電圧信号は復調部９０で復調され演算部１１０に入力される。一方、指紋読取部１００では使用者の指紋データが読み取られ、この指紋データも演算部１１０に入力される。

【００２０】演算部１１０では、データ通信装置１からの送信信号に含まれるＩＤデータ（データ通信装置１の記憶部１０に記憶されていたＩＤデータ）と、演算部１１０に予め登録されたＩＤデータとを照合するとともに、同送信信号に含まれる指紋データ（データ通信装置１の記憶部１０に記憶されていた指紋データ）と指紋読取部１００から出力され、演算部１１０に入力されたた指紋データとを照合して、ＩＤデータの照合結果と指紋データの照合結果とにより使用者を認証する動作が行われる。

【００２１】このように、第１の実施の形態においては、ＩＤデータの照合と指紋データの照合とにより両者照合手段の互いの欠点を補い合い、本人拒否率や他人受入率の低減と「なりすまし」を防止することができるとともに、データ通信装置１から認証装置２へのＩＤデータ、指紋データの伝送を、人体を伝送路とした通信により行っているため、使用者が認証装置２の受信電極７０に触れるだけでデータ伝送を行うことができるという効果を奏する。特に、図２に示すように、認証装置２において、指紋読取部１００と受信電極７０とを互いに近接するように配置すれば、使用者は指紋読取部１００と受信電極７０とに同時に触れて、ＩＤデータによる照合と指紋データによる照合とを同時に行うことができる。よって、非常に簡単な操作で、ＩＤデータによる照合と指紋データによる照合とにより本人認証を行うことができる。

【００２２】尚、データ通信装置１から認証装置２へ人体を伝送路としてデータを伝送を行う基本原理については、本願出願人による特願平１１－１８６００５号に記載されているものと同じである。

【００２３】また、この第１の実施の形態の本人認証システムは、キャッシュカードやクレジットカードの代替ばかりでなく、入退室管理システム、各種キーレスエントリー、コンピュータや携帯端末（携帯電話を含む）のセキュリティ等にも用いることができる。

【００２４】図３は、本発明の第２の実施の形態の本人認証システムを示すのブロック図であり、図３（ａ）は本人認証システムのデータ通信装置を示すブロック図、図３（ｂ）は本人認証システムの認証装置を示すブロック図である。

【００２５】図３（ａ）に示すごとく、データ通信装置１は、第１の実施の形態（図１（ａ））の構成に、データ通信装置１の電極２０及び電極３０の間の電圧もしくは、電極２０及び電極３０のいずれかの一方の電極とデータ通信装置１の回路グランドとの間の電圧を検出する電圧検出部４５と、電圧検出部４５で検出した信号を復調する復調部５５とを付加するとともに、制御部６０には復調部５５からの復調データを記憶部に入力する機能を付加して、認証装置２からの送信データを受信できるようにしている。また図３（ｂ）に示すごとく、前記認証装置２は、第１の実施の形態（図１（ｂ））の構成に、受信電極７０と認証装置２の回路グランドとの間に電圧を印加する電圧印加部８５と、演算部１１０からの信号を変調し電圧印加部８５に変調信号を出力する変調部９５とを付加して、認証装置２からデータを送信できるようにしている。

【００２６】この第２の実施の形態の構成によれば、使用者が認証装置２の受信電極７０に触れると、認証装置２の演算部１１０において保有もしくは登録されている各種のデータが変調部９５で変調され、この変調信号が電圧印加部８５と受信電極７０（ここでは送信に使用する）を介して送信される。データ通信装置１では、認証装置２からの送信信号が電極２０及び電極３０で受信され（ここでは受信に使用する）、この受信信号が電圧検出部４５で電圧信号として検出され、この電圧信号は復調部５５で復調され制御部６０により記憶部１０に入力される。つまり、第１の実施の形態の動作に加え、認証装置２からデータ通信装置１へのデータ伝送も行うことができる。言い換えれば、データ通信装置１と認証装置２とにおいてデータの双方向通信を行うことができる。

【００２７】このようにデータの双方向通信ができるので、本人認証を行った後、データ通信装置１と認証装置２との間で、様々なデータのやり取りを行うことができるという効果を奏する。これにより、電子マネーのやり取りや機密情報のやり取り等、重要な情報のやり取りを、確実に本人認証を行った上でできるようになり、使用者にとっては安心である。また、データ通信装置１（記憶部１０）における指紋データの初期登録を、認証装置２（指紋読取部１００）で読み取った指紋データをデータ通信装置１に送信することで行うことができる。

【００２８】尚、本実施形態では、データ通信装置１の電極２０及び電極３０との間の電圧を電圧検出部４５で検出するようにしているが、電極２０及び電極３０のいずれか一方の電極とデータ通信装置１の回路グランドとの間の電圧を検出するようにしてもよい。また、認証装置２からデータ通信装置１へ人体を伝送路としてデータを伝送を行う基本原理については、本願出願人による特願平１１－３３９１３１号に記載されているものと同じである。

【００２９】さらに、この双方向のデータ伝送が可能な

第２の実施の形態の本人認証システムは、電子マネーによる決済システム、電子化免許証、電子化健康保険証等、ＩＣカードで想定されている各種用途に用いることができる。

【００３０】図４は、本発明の第３の実施の形態の本人認証システムのデータ通信装置を示すブロック図である。本実施形態では、データ通信装置１の電極２０及び電極３０の間を流れる電流量がある定められた値となるように、電極２０及び電極３０に印加する電圧値を制御する定電流制御部１２０を設けている。人体や、人体と電極との界面のインピーダンス成分は、個人毎や部位によって異なり、また同一人物の同一部位でもその時々の皮膚の状態によって異なる。すなわち、同じ電圧印加を行っていても、流れる電流量が変わってしまうことになり、その電流量があまりに少ない場合には、データ通信ができなくなることがある。そこで、電圧印加部４０に電極２０と電極３０との間を流れる電流量がある定められた値となるように電圧値を制御する定電流制御部１２０を設けることによって、個人や部位や皮膚状態等による差が吸収できるようになり、より安定したデータ通信が可能となる。また、このような印加電圧値の制御は、安全性の観点からも重要である。つまり、あまり多くの電流が人体を流れると危険であるため、ここで、定電流制御部１２０において電流値を安全な範囲内に設定しておくことにより、人体に対する安全性を確保することができる。

【００３１】尚、ここでは、定電流制御部１２０を第２の実施の形態のデータ通信装置１に適用しているが、第１の実施の形態のデータ通信装置１に適用してもよい。

【００３２】図５は、本発明の第４の実施の形態の本人認証システムの認証装置の外形図である。本実施形態では、指紋読取部１００を光学的手段により指紋を読み取るものとし、認証装置２の受信電極７０にＩＴＯ（Indium Tin Oxide：インジウム錫酸化物）等の透明電極を用い、指紋読取部１００の上に受信電極７０を重ね合わせるように配置して、受信電極７０（透明電極）を介して、指紋読取部１００で指紋を読み取るようにしている。このようにすることにより、使用者が指紋読取部１００に指を置くだけで、ＩＤデータの照合と指紋データの照合との両方が同時になされて本人認証を行うことができる。

【００３３】さらに、本発明の各実施の形態において、データ通信装置１の記憶部１０に記憶させておく指紋データを圧縮したデータ、あるいは、指紋の特徴（分岐や途切れ等）を示す簡易化されたデータとしてもよい。このようにすることにより、指紋データのデータ量が少なくなり、メモリ容量が少なくなるばかりでなく、データ通信にかかる時間も短縮することができるようになる。また、指紋データを暗号化したデータとしてもよい。このようにすることにより、よりセキュリティ性を高くすることができる。

【００３４】

【発明の効果】上述の如く、本発明の請求項１記載の発明によれば、人の固有データの照合と前記人の生体データの照合とにより本人認証を行う本人認証システムにおいて、前記人の固有データ及び前記人の生体データとしての指紋データを記憶する記憶部と、前記人の体に面するように配置した２つの電極と、該２つの電極間に電圧を印加する電圧印加部と、前記記憶部のデータの入出力制御を行う制御部と、該制御部からの出力信号を変調し前記電圧印加部に変調信号を出力する変調部とを有するデータ通信装置と、前記２つの電極からの信号を受信する受信電極と、前記人の指紋を読み取る指紋読取部と、前記受信電極の受信信号を検出する電圧検出部と、該電圧検出部で検出された受信信号を復調する復調部と、該復調部から出力される前記固有データと登録された固有データとを照合するとともに、該復調部から出力される前記指紋データと前記指紋読取部から出力される指紋データとを照合して、前記固有データの照合結果と前記指紋データの照合結果とにより前記人を認証する演算部を有する認証装置とを具備するようにしたので、簡単な操作で、データ照合と生体認証の両方による本人認証を行うことができる本人認証システムを提供することができた。

【００３５】請求項２記載の発明では、前記認証装置において、前記受信電極と前記認証装置の回路グランドとの間に電圧を印加する電圧印加部と、前記演算部からの信号を変調し該電圧印加部に変調信号を出力する変調部とを付加し、前記データ通信装置において、前記データ通信装置の前記２つの電極間の電圧もしくは、前記２つの電極のいずれかの一方の電極と前記データ通信装置の回路グランドとの間の電圧を検出する電圧検出部と、該電圧検出部で検出した信号を復調する復調部とを付加するとともに、前記制御部には該復調部からの復調データを前記記憶部に入力する機能を付加して、前記認証装置のデータを前記データ通信装置に伝送可能としたので、データ通信装置と認証装置間でデータの双方向通信ができ、本人認証を行った後、データ通信装置と認証装置との間で、様々なデータのやり取りを行うことができるという効果を奏する。

【００３６】請求項３記載の発明では、前記データ通信装置において、前記２つの電極間に流れる電流量を所定の値になるように前記電圧印加部を制御する定電流制御部を設けたので、個人や部位や皮膚状態等による差が吸収できるようになり、より安定したデータ通信が可能となるとともに、人体に対する安全性を確保することができるという効果を奏する。

【００３７】請求項４記載の発明では、前記認証装置において、前記指紋読取部が光学的手段により指紋を読み取る光学式指紋読取部であり、前記受信電極が透明電極

であり、該透明電極を介して、前記光学式指紋読取部で指紋を読み取るようにしたので、使用者が指紋読取部に指を置くだけで、ＩＤデータの照合と指紋データの照合との両方が同時になされて本人認証を行うことができるという効果を奏する。

【００３８】請求項５記載の発明では、前記記憶部における指紋データが圧縮されたデータであるので、指紋データのデータ量が少なくなり、メモリ容量が少なくなるばかりでなく、データ通信にかかる時間も短縮することができるという効果を奏する。

【００３９】請求項６記載の発明では、前記記憶部における指紋データが指紋の特徴を示す簡易化されたデータであるので、指紋データのデータ量が少なくなり、メモリ容量が少なくなるばかりでなく、データ通信にかかる時間も短縮することができるという効果を奏する。

【００４０】請求項７記載の発明では、前記記憶部における指紋データが暗号化されたデータであるので、よりセキュリティ性を高くすることができるという効果を奏する。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態の本人認証システムを示すブロック図であり、（ａ）はデータ通信装置を示すブロック図であり、（ｂ）は認証装置を示すブロック図である。

【図２】本発明の実施の形態に係わる認証装置の外形図である。

【図３】本発明の第２の実施の形態の本人認証システム＊を示すブロック図であり、（ａ）はデータ通信装置を示すブロック図であり、（ｂ）は認証装置を示すブロック図である。

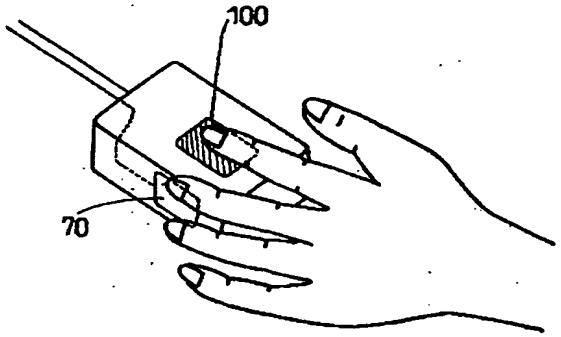
【図４】本発明の第３の実施の形態の本人認証システムのデータ通信装置を示すブロック図である。

【図５】本発明の第４の実施の形態の本人認証システムの認証装置の外形図である。

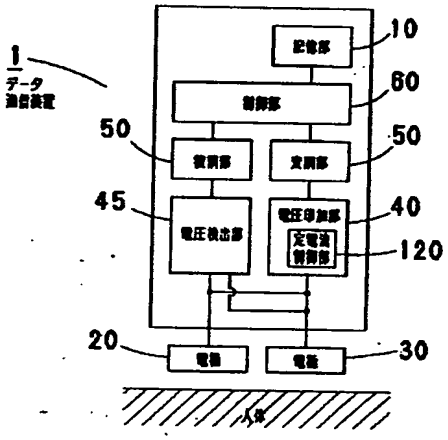
【符号の説明】

１	データ通信装置
２	認証
１０	記憶部
２０	電極
３０	電極
４０	電圧印加部
４５	電圧検出部
５０	変調部
５５	復調部
６０	制御部
７０	（受信）電極
８０	電圧検出部
８５	電圧印加部
９０	復調部
９５	変調部
１００	指紋読取部
１１０	演算部
１２０	定電流制御部

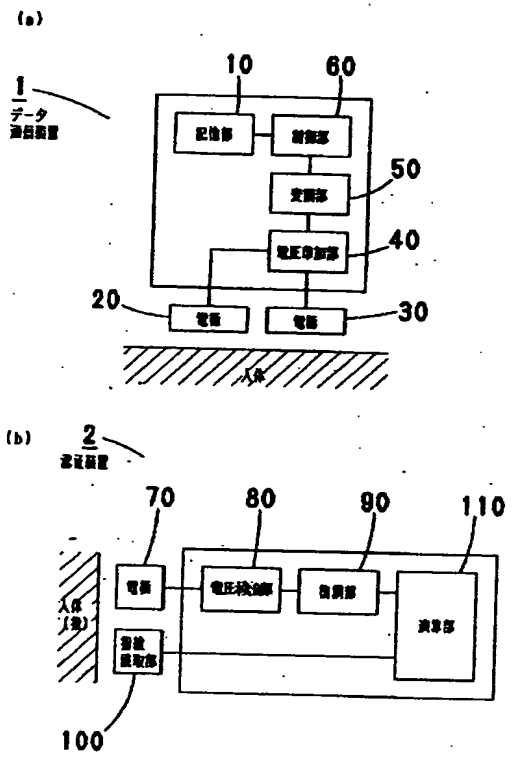
【図２】



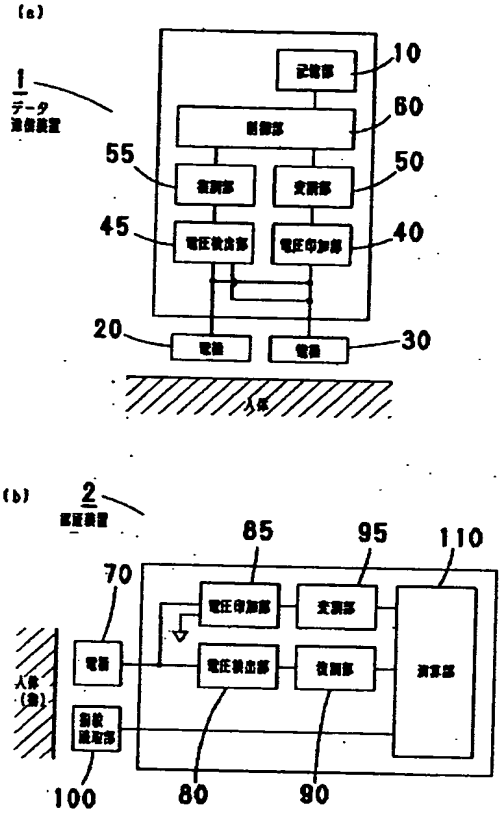
【図４】



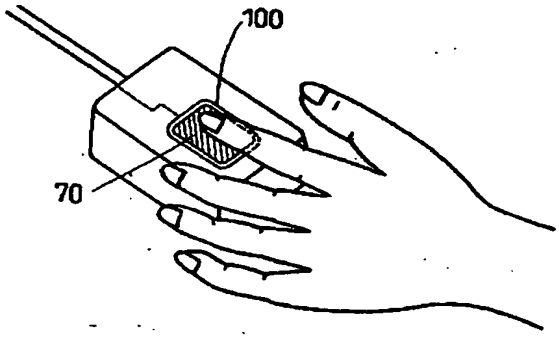
【図１】



【図３】



【図５】



フロントページの続き

(51)Int.Cl.⁷	識別記号	F I	テーマコード(参考)
H04L 9/32		H04L 9/00	673D

(72)発明者 鈴木 佳子
大阪府門真市大字門真1048番地松下電工株式会社内
(72)発明者 西村 篤久
大阪府門真市大字門真1048番地松下電工株式会社内

Ｆターム(参考) 4C038 FF01 FF05 FG00
5B043 AA09 BA02 CA08 FA04 GA01 GA18
5B047 AA25
5B085 AE02 AE26 AE29
5J104 AA07 KA01 KA17 PA02 PA12 PA16